CYBERBIT
TRAIN FOR REAL

Don’t Hire, Train Smarter!

Build Your Internal Cyber Academy Using Cyberbit Range

The global cyber skills crisis has only widened over the course of the year, with over 500,000 cybersecurity jobs remaining unfilled in the US alone according to Cyberseek. Globally, the crisis only worsens with over 4 million open jobs remaining unfilled according to (ISC)2. The global skills crisis has already begun to affect SOC teams with 74% of cybersecurity professionals feeling that their organization has been impacted by a shortage of skilled analysts according to ISSA. As we continue to scale business operations, the need for more skilled cybersecurity professionals is only going to grow. It falls to organizations to develop their own talent rather than search for the "unicorn" candidate with slews of certifications (like CISSP, CompTIAPenTest+, CySA+, CASP+, CEH, CISSP and CISM), long tenures in the industry (10+ or, in some cases, 20+ years of experience, longer than most relevant technology has been around), and specialized skills in not one, but several, tech stacks and disciplines. Cyberbit Range is key in taking novices from "zero to hero" in a time efficient manner, ensuring that your SOC is prepared for any attack.

Salaries Rise, Skills Fall

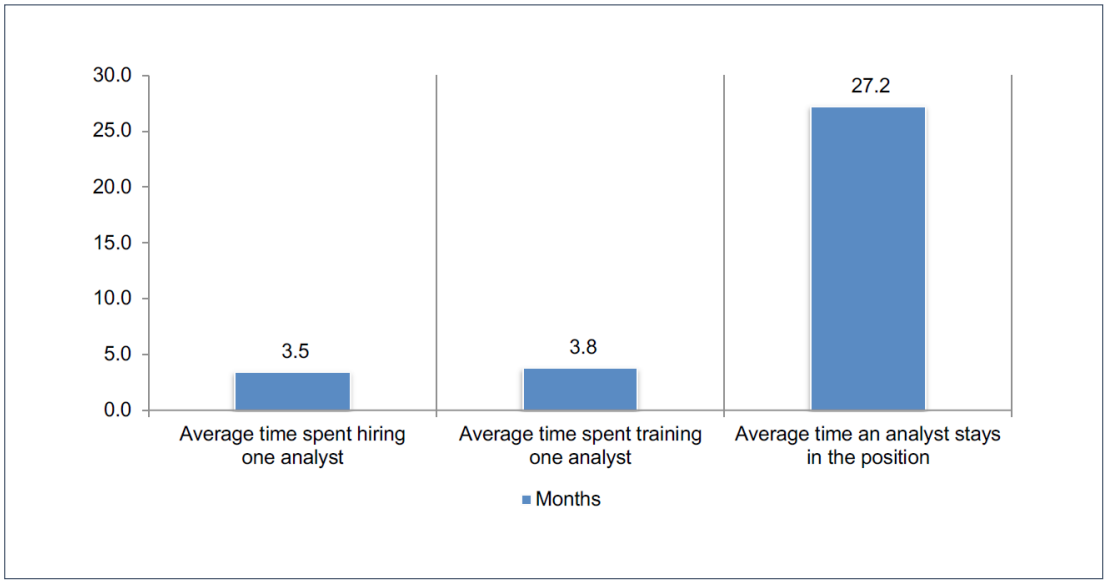
From various interviews held with CISOs around the world, we know that employee salaries is one of the top line items in a cybersecurity budget. Salaries for cybersecurity professionals have risen by 6% in one year, double the national average of 2.9%, according to Acumin Consulting's latest annual Salary Survey. With salaries continuing to rise and talent poaching amongst companies becoming a regular event, hiring cybersecurity professionals with significant experience is becoming significantly more expensive. In fact, there are now 1,262 recruitment agencies globally (Acumin Consulting Salary Survey) contacting cybersecurity professionals who are not looking for a new job an average of at least once a month. The more cybersecurity professionals move around, the larger the demand becomes, the more salaries will continue to rise for the same position, regardless of skill level.

Candidates Exaggerate Skill Level

Candidates send in a CV that represents the best image of themselves. Sometimes that image is a bit exaggerated, often intended to show that the candidate has a higher skill level than they currently possess. Hiring this candidate could and likely will result in a "mis-hire" or a hire that would not have occurred if the correct information had been represented. The high salaries on the table in cybersecurity tend to attract talent that would not be qualified for the job proposed. However, with the cyber skills shortage looming so large, companies rush to hire candidates, fearing a loss to a competing organization. Mis-hires can result in higher cybercrime costs, increased time to detection for critical incidents, and an overall decrease in the skill level of your SOC.

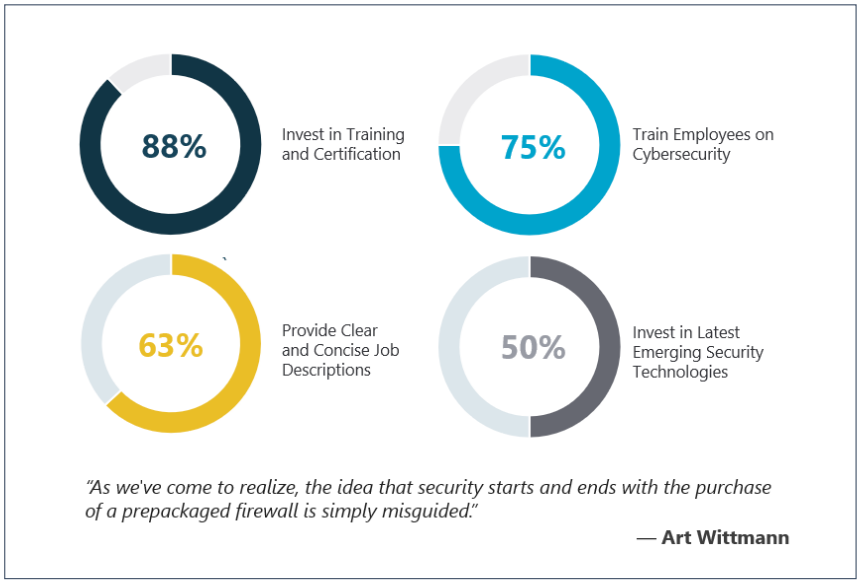
Training is Faster and More Cost Effective than Hiring and Onboarding

According to the Ponemon Institute, companies spend an average of 7 months hiring and training a cybersecurity analyst to work in their SOC. Hiring a candidate with no experience and the right soft skills can be a daunting task but given the upside may sound more enticing. With the right training environment, a candidate with no experience can be ready and operational in under 5 months with a significantly reduced cost to your organization from a salary perspective. This means you can have the same talent level in your SOC more quickly and with a lower cost.



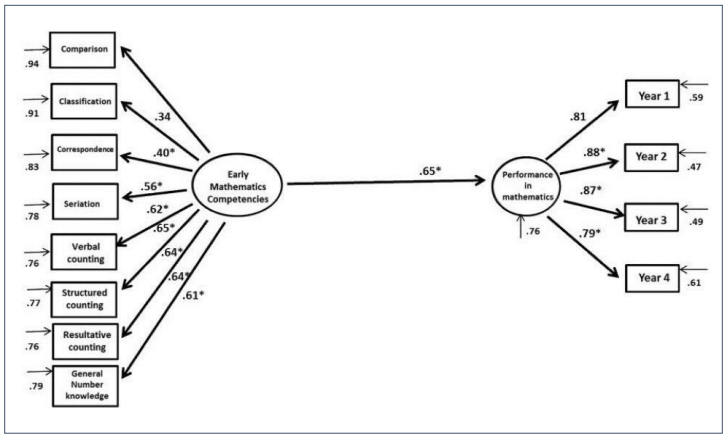
Train Employees to Keep Employees

Training is important to your employees. SOC Team members are aware that the threat landscape is constantly evolving. To keep up with the latest certifications, threat vectors and techniques, and technologies, your team requires advanced training following their introduction into the SOC. In fact, according to (ISC)[2], 88% of cybersecurity professionals prefer employers who invest in training. Your employees are aware of and heavily agree with Art Wittman's statement: "The idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided."



Train Using the Right Methodology

To ensure that your new, untrained, and untested cybersecurity hopefuls can gain the right skills for your SOC as quickly as possible, it is best to train them using the most advanced educational technologies. Cognitive modeling has shown us that using “building blocks” for training and education leads to vastly superior knowledge retention and habit-forming behaviors. In layman’s terms, learn individual skills and then bring them together in a realistic environment. In math, you may recognize this as the multiplication table, beginning small and evolving to more complex equations as simpler skills are mastered. The same theory applies to language processing, sports, and a myriad of learned behaviors. For cybersecurity, this means training simple skills before moving to more complex attack simulations.



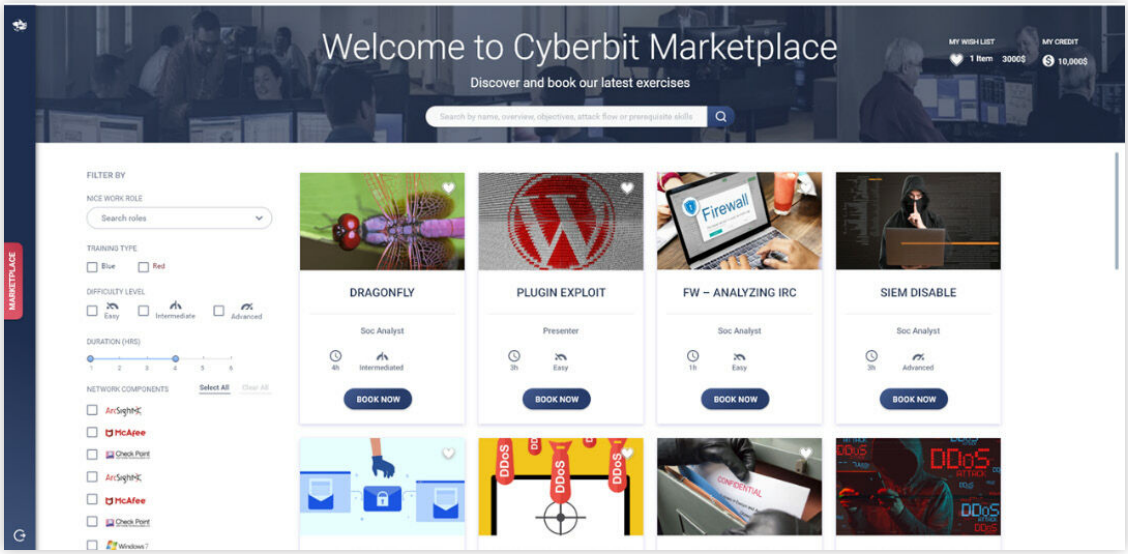
Build Your Internal Cyber Academy with Cyberbit Range

Training, Cross-Training, or Upskilling new cybersecurity candidates, IT Teams, NOC Teams, and other candidates with the right skills can be a daunting and time-consuming process. However, with Cyberbit Range, building an internal cyber academy is achievable with minimal extra resources required.

Cyberbit Range is the only cybersecurity training platform that provides all four elements of an effective skills building program, built on the theories behind educational cognitive modeling:

- Build Foundational Elements with Theoretical Labs
- Enhance Cybersecurity Skills Learning & Practice with Practical Labs
- Apply Cybersecurity Skills Against a Real-World Attack
- Automated Assessment and Feedback

Content on Cyberbit Range is updated constantly to ensure that your trainees are training for the most relevant and recent threat vectors. The above approach has been proven to reduce training time by up to 66% and improve incident response time by as much as 26%.



Training for Specific Roles

Cyberbit Range integrates the NICE Cybersecurity Framework to ensure that SOC Team members are spending their time training for their specific role inside the SOC as outlined by NICE. Career paths included with Cyberbit Range align to specific KSAs associated with each individual role. Each path includes a development process associated with specific theoretical labs, practical labs, and real-world attacks to ensure that your trainee is prepared to join your SOC and contribute to the operational capacity required for their specific work role. Managers track employee and trainee progress to ensure that employees and trainees alike are prepared for the role they are filling in the SOC. For existing employees, progress tracking also allows management to determine who is ready to be promoted given their experience and training level.

Training with Industry Best Practices and Standards

Cyberbit Range ensures your trainees are training to respond according to the NIST Incident Response Framework. Training your team to use the same incident response framework ensures that your team is training with the same response path. Training to respond the same way will reduce miscommunications during incident response, ensure your team understands what the role of other team members are, and ensure that members of your SOC team can fill in for team members if required.

Providing existing and future SOC team members with valuable experience should be a core focus of your internal cyber academy. Measuring the experience that your team has with attacker behavior will allow you to assign the appropriate person to deal with relevant incidents. To ensure that you have enough coverage of attacker behaviors, Cyberbit Range is aligned with MITRE ATT&CK enterprise. Based on your assigned training sessions, Cyberbit Range will automatically track which SOC Team members have experience with specified attacker behaviors, providing you with the required information to assign the right analyst to the right incident.

Train with the Right Tools

The tools your team uses in your security operations center are not open source, unless open source has become the industry standard. Cyberbit Range contains a variety of commercial grade tools (Firewalls, SIEMs, etc.) from top-tier cybersecurity technology providers including Checkpoint, Palo Alto Networks, Splunk, IBM and more. Training using industry standard technology will ensure that your team is familiar with the tools and features used daily inside your SOC. Additionally, training on commercial grade tools will allow you to test different tool types to see which tools your team performs best with, further improving time to response.

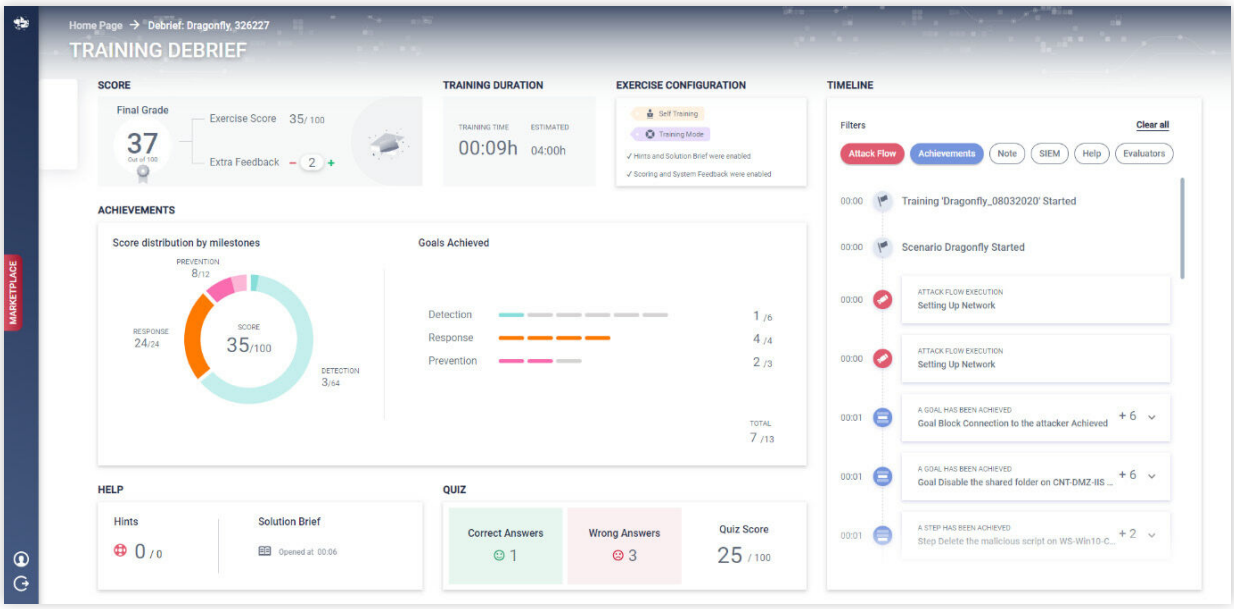
Develop Critical Soft Skills

Cyberbit Range is the perfect environment to assess and develop critical soft skills for your team to be successful in the real world. Experiencing the pressure of a real-world attack will expose your team to pressure, forcing them to display their soft skills in a critical situation. During these sessions you will see your trainees and SOC analysts display leadership skills, see how well they communicate under pressure, determine who can analyze large amounts of data rapidly, and who collapses under the pressure. With this information you can either improve soft skills where required or identify team members who are ready for promotion to team leaders.

Train for Performance

To ensure that your trainees and team improve, you must provide constructive feedback. Let them know where they have missed important steps in attack investigation and mitigation, where they can improve their intra-team communication, and where they are lacking the required knowledge to build a skill. Using the information relayed during a training session, next training steps become clear.

Cyberbit Range includes a complete debriefing suite, providing critical feedback to trainees. Included in the dashboard are goals and milestones achieved based on the NIST Incident Response Framework, Time to Response measurement, where trainees required hints, and how they performed in post exercise quizzes. Each point of measured data included in the debriefing suite has a directly correlated action, allowing you to focus training on problem areas and transforming the aforementioned areas into strengths.



ABOUT CYBERBIT™

Cyberbit provides hands-on cybersecurity education and training and addresses the global cybersecurity skill gap through its world-leading cyber range platform. Colleges and universities use Cyberbit Range to increase student enrollment and retention, train industry organizations, and position their institution as regional cybersecurity hubs by providing simulation-based learning and training. The Cyberbit Range platform delivers a hyper-realistic experience that immerses learners in a virtual security operations center (SOC), where they use real-world security tools to respond to real-world, simulated cyberattacks. As a result, it prepares students for their careers in cybersecurity from day-one after their graduation and reduces the need to learn on the job. Cyberbit delivers over 100,000 training sessions annually across 5 continents. Customers include Fortune 500 companies, MSSPs, system integrators, higher education institutions and governments. Cyberbit is headquartered in Israel with offices in the US, Europe, and Asia.

sales@cyberbit.com | www.cyberbit.com

CYBERBIT
TRAIN FOR REAL